DETAILED ACTION

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this Examiner's Amendment was given in a telephone interview with Benjamin C. Stasa (Reg. No. 55,644) on 2 January 2009.

This application has been amended as follows:

IN THE CLAIMS

Cancel claim 5, 13, 21, 24, 29 – 31, 33 and 34.

Replace claim 1, 2, 8, 10, 14, 17, 19, 20, 25, 27, 32, 35 and 36 as follows.

Claim 1:

A method for transmitting data according to a signature-based protocol comprising:

generating, at a server and in response to a request from a nonsigning client device, a signature corresponding to a signature block~~, the signature block~~ having a covered data portion and an information object portion, the signature computed only on data in the covered data portion such that payload data is not included in computing the signature, the server conversant in a predetermined protocol and the signature and signature block ~~being~~ conformant with the predetermined protocol;

storing, at the server, the signature in the signature block, the signature covering the covered data portion and the information object portion remaining independent of the signature;

transmitting, from the server to the nonsigning ~~a remote~~ client device ~~also conversant in the predetermined protocol~~, the signature block, the ~~remote client being a~~ nonsigning client device conversant in the predetermined protocol and unable to generate the signature in the signature block, the signature block further operable to store, in the information object portion, payload data in a nondestructive manner ~~the nondestructive manner operable~~ so as to preserve the covered data portion and corresponding signature generated by the server without regenerating the signature ~~such that the payload data is not included in computing the signature~~, the covered data portion remaining unwritten by the nonsigning client device; and

storing, at the nonsigning client device, ~~in the information object portion further comprising storing the~~ payload data in the information object portion ~~at the remote client~~, ~~the nonsigning remote client being unencumbered by signature generation operability,~~ the signature block receivable by a recipient destination having capability to authenticate the signature and ~~,~~ ~~the recipient destination further~~ conversant in the predetermined protocol.

Claim 2:

The method of claim 1 wherein the signature block further includes a signature value portion, the signature value portion operable to store the signature as an authentication indicator according to the predetermined protocol, wherein storing further comprise storing the signature in the signature value portion.

Claim 8:

The method of claim 1 further comprising computing a digest on the covered data portion, the digest ~~substantially~~ indicative of the data in the covered data portion.

Claim 10:

A method for transmitting data from a nonsigning client device according to a signature-based protocol[[,]] comprising:

receiving, at a nonsigning client device, a signature block and a signature corresponding to the signature block generated by a server in response to a request from the nonsigning client device, the signature block having an information object portion and a covered data portion corresponding to the signature~~, and an information object portion~~, the signature computed only on data in the covered data portion such that payload data is not included in computing the signature, the ~~receiving performed by a~~ nonsigning client device unable to ~~which does not~~ compute the signature and ~~is unencumbered by components operable to compute the signature, the receiving client~~ conversant in a predetermined protocol, [[and]] the signature and signature block being conformant with the predetermined protocol;

storing, at the nonsigning client device and in the information object portion of the signature block, payload data in a nondestructive manner so as ~~the nondestructive manner operable~~ to preserve the covered data portion and the corresponding signature generated by the server without regenerating the signature ~~such that the payload data is not included in computing the signature~~, the signature covering the covered data portion and the information object portion remaining independent of the signature, the covered data portion remaining unwritten by the nonsigning client device; and

transmitting, from the nonsigning client device to a recipient destination conversant in the predetermined protocol ~~according to the predetermined protocol~~, the signature block according the predetermined protocol ~~to a recipient destination conversant in the predetermined protocol~~, the information object portion included in the signature block according to the predetermined protocol, the signature block including the public key corresponding to a private key employed in generating the signature, the included public key thus providing a self-authentication message for delivery to the recipient destination.

Claim 14:

The method of claim 10 wherein receiving the signature further comprises indexing a remote signature repository, and the nonsigning client device is further operable to store the received signature in the signature block according to the predetermined protocol.

Claim 17:

The method of claim 10 [[13]] further comprising:

receiving, at the nonsigning client device, a plurality of signatures and corresponding covered data portions;

selecting a first signature for inclusion in a first signature message for transmission to a destination recipient; and

selecting a second signature different than the first signature for inclusion in a second signature message for transmission to the same destination recipient.

Claim 19:

The method of claim 18 wherein the signature selection logic is operable for analyzing the covered data portion based on at least one of [[the]] content type, size, creation date, and sparsity of the data.

Claim 20:

A data communications device for transmitting data according to a signature-based protocol comprising:

a cryptographic engine operable to generate, by a server in response to a request from a nonsigning client device, a signature corresponding to a signature block, the signature block having a covered data portion and an information object portion, the signature computed only on data in the covered data portion such that payload data is not included in computing the signature, the server conversant in a predetermined protocol and the signature and signature block being conformant with the predetermined protocol;

a metalanguage processor conversant in the predetermined protocol and operable to store the signature in the signature block, the signature block further including a signature value portion, the metalanguage processor further operable to store, in the signature value portion, authentication indicators according to the predetermined protocol, wherein storing further comprise storing the signature in the signature value portion; and

an interface in the data communications device operable to transmit, according to the predetermined protocol, the signature block to a the nonsigning client device conversant in the predetermined protocol and unencumbered by signature generation operability, the metalanguage processor being further operable to generate the signature block having the information object portion, the information object portion further operable for storing the payload

data at the nonsigning client device ~~unencumbered by signature generation operability~~, the signature block further operable to receive and store, in the information object portion, payload data in a nondestructive manner so as ~~the nondestructive manner operable~~ to preserve the covered data portion and corresponding signature generated by the server without regenerating the signature ~~such that the payload data is not included in computing the signature~~, the signature block being a script having fields defined by a predetermined metalanguage syntax, the metalanguage syntax defining the position of the covered data portion and corresponding signature, the signature block receivable by a recipient device conversant in the predetermined metalanguage syntax for decoding the message.

Claim 25:

The data communications device of claim 20 wherein the signature block is adapted for storing the payload data by the nonsigning client device to generate a signature message transmission block of data conformant with the predetermined protocol and operable to be received as a signature authenticated transmission by a destination node according to the predetermined protocol.

Claim 27:

The data communications device of claim 20 wherein the cryptographic engine is further operable to compute a digest on the covered data portion, the digest ~~substantially~~ indicative of the data in the covered data portion.

Claim 32:

A computer program product having an encoded set of processor based instructions defined as computer program code on a computer readable storage medium operable to store computer program logic embodied in computer program code encoded thereon for transmitting data from a nonsigning client device according to a signature-based protocol comprising:

computer program code for receiving, at the nonsigning client device, a signature block and a signature corresponding to the signature block generated by a server in response to a request from the nonsigning client device, the signature block having an information object portion and a covered data portion corresponding to the signature, ~~and an information object portion,~~ the signature computed only on data in the covered data portion such that payload data is not included in computing the signature, the receiving nonsigning client device conversant in a predetermined protocol and the signature and signature block being conformant with the predetermined protocol;

computer program code for storing, in the information object portion of the signature block, payload data in a nondestructive manner so as ~~the nondestructive manner operable~~ to preserve the covered data portion and the corresponding signature generated by the server without regenerating the signature ~~such that the payload data is not included in computing the signature~~, the covered data portion remaining unwritten by the nonsigning client device, wherein storing in the information object portion further comprises storing the payload data in the information object portion at the nonsigning [[a]] client device, the nonsigning client device being unencumbered by signature generation operability; and

computer program code for transmitting, according to the predetermined protocol, the signature block to a recipient destination conversant in the predetermined protocol, the information object portion included in the signature block according to the predetermined

protocol, wherein the signature block further includes a signature value portion, the signature value portion operable to store the signature as an authentication indicator according to the predetermined protocol, wherein storing further comprises storing the signature in the signature value portion, the signature covering the covered data portion and the information object portion remaining independent of the signature, the signature block being a script having fields defined by a predetermined metalanguage syntax, the metalanguage syntax defining the position of the covered data portion and corresponding signature, the signature block receivable by a recipient device conversant in the predetermined metalanguage syntax for decoding the message.

Claim 35:

The method of claim 1 further comprising:

generating, at the server, a set of predetermined signatures operable for insertion in a message conformant to the predetermined protocol;

storing, in a signature repository at the server, a bank of signatures including the set of predetermined signatures; and

transmitting, responsive to a request from the nonsigning client device, a signature from the bank of signatures for insertion in a signature block in conjunction with a payload.

Claim 36:

A method for transmitting data in conformance with a signature-based protocol comprising:

transmitting, from a nonsigning client device to a server, a request for a signature block, ~~the signature block~~ operable to store signature based data corresponding to a predetermined protocol;

generating, at the server, a signature block~~, the signature block~~ having a covered data portion corresponding to a signature and an information object portion for storing payload data ~~independent of the signature, the covered data portion corresponding to a signature and the information object portion for storing payload data independent of the signature~~;

computing, at the server ~~based on the covered data portion~~, a signature ~~indicative of the covered data portion~~ based only on the covered data portion such that payload data is not included in computing the signature~~, the signature computed only on data in the covered data portion~~;

storing, at the server, the computed signature in the signature block ~~before writing to the information object portion~~;

transmitting, from the server to the nonsigning client device, the signature block ~~to the nonsigning client~~, the nonsigning ~~non-signing~~ client device conversant in the predetermined protocol and unable ~~but absent an ability~~ to compute and authenticate the signature ~~indicative of the covered data portion~~;

populating, at the nonsigning client device ~~after receiving the signature block~~, the information object portion of the signature block with payload data without destroying and regenerating the signature, the information object portion independent of the signature generated by the server, the populating preserving the covered data portion and the corresponding computed signature according to the predetermined protocol such that the populating is not included in computing the signature, the covered data portion remaining unwritten by the nonsigning client device; and

transmitting, from the nonsigning client device to a destination, the signature block, the ~~to a~~ destination operable to (i) receive and authenticate the signature and corresponding

covered data portion and (ii), ~~the destination further operable to~~ receive the payload data in the information object portion.

Allowable Subject Matter

Claims **1 – 4, 6 – 12, 14 – 20, 22, 23, 25 – 28, 32 and 35 – 37** are allowed.

The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations recited in claims 1, 10, 20, 32 and 36 (& associated dependent claims).

The present invention is directed to a method for transmitting data according to a signature-based protocol. No singular art disclosing, nor motivation to combine has been found to anticipate or render obvious the claimed invention of generating, at a server and in response to a request from a nonsigning client device, a signature corresponding to a signature block having a covered data portion and an information object portion, the signature computed only on data in the covered data portion such that payload data is not included in computing the signature, the server conversant in a predetermined protocol and the signature and signature block conformant with the predetermined protocol; storing, at the server, the signature in the signature block, the signature covering the covered data portion and the information object portion remaining independent of the signature; transmitting, from the server to the nonsigning client device, the signature block, the nonsigning client device conversant in the predetermined protocol and unable to generate the signature in the signature block, the signature block further operable to store, in the information object portion, payload data in a nondestructive manner so as to preserve the covered data portion and corresponding signature generated by the server without regenerating the signature, the covered data portion remaining unwritten by the

nonsigning client device; and storing, at the nonsigning client device, payload data in the information object portion the signature block receivable by a recipient destination having capability to authenticate the signature and conversant in the predetermined protocol.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Primary Patent Examiner
Art Unit 2431
1/2/2009